In the Claims

1. (Currently Amended) ~~In a~~ A method of enforcing geographical restrictions on content redistribution in a TCP/IP network, ~~an improvement~~ comprising:

defining a geographical boundary across which certain content does not pass, wherein said boundary is defined – at least in part – by a hardware firewall device; and

determining whether an IP packet should be regarded as conveying content that should not cross said boundary, by reference to one or more flag bits included in the header of said packet;

wherein said one or more flag bits are related to the payload of a watermark in the content.

2-3. (Canceled)

4. (Currently Amended) ~~In a~~ A method of data processing that includes forming an IP packet having header data and body data, wherein the header data includes a first destination address, ~~an improvement~~ **the method** comprising:

forming said header data to additionally include additional data specifying whether it is permissible to send a copy of data in the packet to a second destination address**, wherein the additional data has at least two states, respectively indicating:**

(a) it is not permissible to send a copy of data in the packet to any second destination address; or

(b) it is not permissible to send a copy of data in the packet to any second destination address except to a second destination address within a domain that also includes the first destination address; and

wherein said domain comprises networked devices associated with a single family.

5-6. (Canceled)

7. (Original) The method of claim 4 wherein a device associated with the first destination address has a first physical location and a device associated with the second destination address has a second physical location, and the additional data includes a field signaling that copying of data in said packet to said second destination address should be:

(a) permitted if the second physical location is physically proximate to the first physical location; and

(b) prohibited if the second physical location is physically remote from the first physical location.

8. (Original) The method of claim 7 wherein the first and second destination addresses are within a common domain.

9. (Original) The method of claim 7 wherein the first and second destination addresses both correspond to network devices associated with a single family.

10. (Original) The method of claim 4 wherein said additional data is related to the payload of a watermark encoded in the body data.

11. (Currently Amended) ~~In a~~ **A** method of data processing that includes receiving an IP packet having header data and body data, wherein the header data includes a first destination address, the first destination address corresponding to a device at a first physical location proximate to where said method is practiced, ~~an improvement~~ **the method** comprising interpreting additional data in the header of said packet as specifying whether it is permissible to send a copy of data in the packet to a second destination address**, wherein:**

(a) if the additional data has a first state, prohibiting transmission of a copy of data in the packet to any second destination address; and

(b) if the additional data has a second state, prohibiting transmission of a copy of data in the packet to any second destination address other than a second destination address within a domain that also includes the first destination address.

12. (Canceled)

13. (Currently Amended) The method of claim ~~[[12]]~~ **11**, wherein said domain comprises networked devices associated with a single family.

14. (Original) The method of claim 11 wherein a device associated with the second destination address has a second physical location and wherein:

(a) if the second physical location is physically proximate to the first physical location, permitting copying of data in said packet to the second destination address; and

(b) if the second physical location is physically remote from the first physical location, prohibiting copying of data in said packet to the second destination address.

15. (Original) The method of claim 14 wherein the first and second destination addresses are within a common domain.

16. (Original) The method of claim 14 wherein the first and second destination addresses both correspond to network devices associated with a single family.

17. (Original) The method of claim 14 wherein the method includes determining whether the second physical location is physically remote from the first physically location by reference to whether the second destination address is served by a common firewall with the first destination address.

18. (Original) The method of claim 11 wherein said additional data is related to the payload of a watermark encoded in the body data.

19. (Original) A method wherein content is divided and collectively represented by plural packets of data, each packet having first and second portions, the first portion of each packet including a divided part of the content, the method including obtaining an identifier of said content, and including said content identifier in the second portion of each packet.

20. (Original) The method of claim 19 wherein said obtaining includes examining a previous representation of said content that has an identifier associated therewith.

21. (Original) The method of claim 19 wherein the packets comprise IP packets, each having a body portion as said first portion, and a header portion as said second portion, said header portion including address information in addition to said content identifier.

22. (Original) The method of claim 19 wherein the packets comprise non-contiguous blocks of data in a storage medium, said blocks being associated together by a table of file allocation data.

23. (Original) The method of claim 22 wherein each of said non-contiguous blocks includes a content identifier, but data in said table does not.

24. (Original) The method of claim 19 that further includes reading the content identifier from the second portion of one of said packets to identify content represented by data in the first portion.

25. (New) A method of deterring unauthorized redistribution of video entertainment from a consumer's home network, the consumer's home network employing at least a computing device and a networking device;

wherein acts performed by the computing device include:

ascertaining restriction information for the video entertainment, said ascertaining including at least one of: (a) extracting restriction information from header data conveyed with the video entertainment; (b) obtaining restriction information from a remote repository associated with the video entertainment; or (c) discerning the restriction information by reference to data decoded from digital watermark information hidden within the video entertainment;

dividing the video entertainment among payload portions of plural IP packets;

including data indicating said ascertained restriction information in header portions of each of said IP packets; and

sending the packets to the networking device;

and wherein acts performed by the networking device comprise examining said included data and refusing to transmit the packets through the networking device to a different network if the included data indicates that the video entertainment should not be redistributed from the consumer's home network.

26. (New) The method of claim 25 wherein the ascertaining includes extracting restriction information from header data conveyed with the video entertainment.

27. (New) The method of claim 25 wherein the ascertaining includes obtaining restriction information from a remote repository associated with the video entertainment.

28. (New) The method of claim 25 wherein the ascertaining includes discerning the restriction information by reference to data decoded from digital watermark information hidden within the video entertainment.